



# **Annual Privacy Act Refresher Training 2015**

**Protecting Personally Identifiable  
Information (PII)"**



# ANNUAL PRIVACY ACT TRAINING

- This annual refresher training is required under ALNAV 070/07 to ensure all employees understand their responsibilities for the protection of personal information under the Privacy Act.
- This training seeks to establish a culture of sensitivity to, and knowledge about, privacy issues involving individuals throughout the DOD and its component agencies.
- This training should take approximately 20 minutes.
- If you are not currently logged in using your Common Access Card (CAC), you will need to submit a printed and signed copy of your course completion certificate to your Administrative Officer. Otherwise, your CAC card is your electronic signature of completion. The certificate is provided at the end of this training.



# **You Need To Know About Privacy Because –**

- **It's information we collect, maintain, distribute and dispose of about you.**
- **It requires you to take precautions when collecting, maintaining, distributing, and disposing of PII as required by your job.**
- **It's a factor in developing best business practices.**
- **It contains both civil and criminal penalties for non-compliance.**



# What is the Privacy Act?

The Privacy Act of 1974 is a Federal Law that limits an agency's collection and sharing of personal data. The Privacy Act focuses on four basic policy objectives:

1. To restrict disclosure of personally identifiable records maintained by agencies.
2. To grant individuals increased rights of access to agency records maintained on themselves.
3. To grant individuals the right to seek amendment of agency records maintained on themselves upon a showing that the records are not accurate, relevant, timely, or complete.
4. To establish a code of "fair information practices," which requires agencies to comply with statutory norms for collection, maintenance, and dissemination of records.



# What is a Record?

**A record is any item, collection or grouping of information about an individual, whatever the storage media (e.g., paper, electronic, etc.), that is maintained by an NRL activity including, but not limited to, the individual's education, financial transactions, and medical, criminal or employment history, and that contains the individual's name or other identifying particulars assigned to the individual, such as an employee number, finger or voice print or photograph.**



# What is a System of Records?

- **A System of Records is a group of records that:**
  - Contains a personal identifier (such as a name, Social Security Number, Employee number, etc.)
  - Contains one other item of personal data (such as home address, performance rating, blood type, etc.), and
  - Is retrieved by a personal identifier.



# System Of Records Notice (SORN)

- If you collect or retrieve information from a “system of records,” you must follow specific rules and procedures that authorize and safeguard PII collected under that system.
- A Privacy Act (PA) System of Records Notice (SORN) is a "blueprint" for the kinds of information that may be collected, maintained and disseminated under a specific system of records.
- It provides the keeper of the system and the subject of the system with specific information on what may be contained in the system of records.



# The SORN Sets The Rules

- **More specifically, it identifies:**
  - the kind of information being collected and on whom,
  - the authority for collecting the information,
  - where it is located and how it is filed,
  - to whom it is routinely disclosed,
  - how to access the information contained in the system,
  - how long the information will be maintained, and
  - where (from whom) the information was obtained.
- **Do you know what “SORN” governs the personal information you collect or manage?**



## SORN (cont.)

- Every federal system of records is required to have an approved, updated SORN published in the Federal Register.
- NRL systems generally fall under “umbrella” Privacy Act systems established by another Federal agency, such as the DON or OPM.
- Umbrella systems are generic systems of records that can be used by anyone in the Navy or other government activity, for the purposes authorized in the approved notice.

**Note:** Examples of commonly used DON umbrella systems are NM05000-1, General Correspondence Files and NM05000-2, Program Management and System Locator.



# Definition of Personally Identifiable Information (PII)

- **PII – “...information about an individual that identifies, links, relates, or is unique to, or describes him or her, e.g., a SSN; age; rank; grade; marital status; race; salary; home/office phone numbers; other demographic, biometric, personnel, medical and financial information.” DoD Memo 21 Sep 07**



# Sensitive PII

## What is sensitive PII?

- Sensitive PII is defined as PII which, when disclosed, could result in harm to the individual whose name or identity is linked to the information.
- Sensitive PII must be securely handled, processed, and transmitted, and must always be treated as “For Official Use Only,” and marked accordingly. This applies to conventional records, as well as electronic transmissions (including emails) and faxes.



# Sensitive PII

**What data elements are considered sensitive PII?**

**Data elements, when grouped with a person's name or other unique identifier, result in sensitive PII such as the following:**

- **Citizenship or immigration status (Note: While citizenship is considered sensitive PII, it is not in the following instances/contexts: foreign national badges, NRL's Locator system, and email ID.)**
- **Medical information**
- **Driver's license number**
- **Passport number**
- **Full date of birth**
- **Authentication information, such as mother's maiden name**
- **Portions of SSNs, such as last four digits**
- **Financial information, such as account numbers**
- **Leave balances; types of leave used**
- **Drug test results and the fact of participation in rehabilitation programs**
- **Religion, race, national origin**
- **Performance ratings**



# Sensitive PII

- Context also matters –

**Even if a data element itself is not otherwise considered sensitive PII, the context of the data element must be considered. For example, while a folder containing a list of attendees at a public meeting would not be considered sensitive PII, a folder containing a list of employees who tested positive during random drug testing would be.**

- And stand-alone data elements –

**Some categories of PII are sensitive as stand-alone data elements. In and of themselves they are considered sensitive PII whether grouped with other data elements or not. Examples include: Social Security Numbers (SSNs) and biometric identifiers (fingerprint, iris scan, voice print, etc.)**



# Non-sensitive PII

**Not all PII is sensitive –**

- **Examples of non-sensitive PII include –**
  - Job title
  - Pay grade
  - Office phone number
  - Office address
  - Office email address
- **What does this mean? Most business-related PII when lost, stolen, or compromised is not cause for submission of a PII breach report ...**



# PII Breach

## What is a PII breach?

- A breach is defined by the Office of Management & Budget as:

**A loss of control, compromise, unauthorized disclosure, unauthorized acquisition, unauthorized access, or any similar term referring to situations where persons other than authorized users and for an other than authorized purpose have access or potential access to personally identifiable information, whether physical or electronic.**

- This includes, but is not limited to, posting PII on public websites; sending via e-mail to unauthorized recipients; loss of electronic devices or media storing PII (for example, laptops, thumb drives, compact discs, etc.); and all other unauthorized access to PII.



# Hold Your Breaches

***“On 5 Jan. 2008, a government employee was notified by the local police that “someone had stolen his identity and was about to use his credit card to buy a big screen TV at a major department store.” One of the suspects arrested possessed a two-page report dated 1994 containing government employment data. That same individual had other credit cards, four of which related to names in the compromised report. The report contained names, Social Security numbers, date of birth, organization code, position title and other employment related data. It is unknown how they came to be in possession of this hard copy report and whether additional pages of this report had also been compromised.”***



# Lessons Learned

- ✓ **Compromised PII data can be used by thieves for many years to come.**
- ✓ **Wherever possible, delete Social Security numbers and sensitive personal information from any list, database or e-mail before transmission or storage. SSNs are a critical element used in stealing personal identity.**
- ✓ **Routinely review files and destroy PII by making it unrecognizable when no longer needed.**



# Social Security Numbers

## Social Security Numbers – a special case

- The SSN is the most frequently lost, stolen, or compromised PII data element, and human error is the cause of 80 percent of the DON's PII breaches.
- SSNs are improperly disclosed by: 1) sending SSNs in an email or attachment, 2) creating recall rosters with SSNs, or 3) posting names with associated SSNs to web portals or shared drives.
- The DoD and DON are working to eliminate the unnecessary collection of SSNs to protect PII.
- OMB (Office of Management and Budget) M-07-16 memorandum entitled Safeguarding Against and Responding to the Breaches of Personally Identifiable Information, issued in 2007, called for agencies to, among other requirements, review current PII holdings and reduce them to the minimum necessary to properly perform a documented agency function. It also called for agencies to reduce the unnecessary use of SSNs and explore alternatives to agency use of SSNs as personal identifiers.



# Your Responsibilities

**If you collect, maintain, or use PII, it must support a DON function or program as authorized by law, Executive Order, or operational necessity. Whether you are working from your desk at the office, at home, or in the field, it is your responsibility to:**

- Ensure that the information entrusted to you in the course of your work is kept secure and protected.
- Minimize the use, display, or storage of SSNs and other PII whenever possible.
- Keep the information timely, accurate and relevant to the purpose for which it was collected.
- Allow only those personnel with “a need to know” access to PII.
- Immediately notify your Privacy Act Coordinator and/or supervisor if you suspect or discover that PII has been lost or compromised.



# Privacy Act Rules Of Conduct

## From NRLINST 5211.2F, PRIVACY ACT POLICY AND RESPONSIBILITIES

1. Maintaining Personal Records. It is unlawful to maintain a system of records about individuals without prior announcement in the Federal Register. Anyone who does is subject to criminal penalties and a fine up to \$5,000. Even with such notice, care shall be taken to keep only such personal information as is necessary to do what law and the President, by Executive order, require. The information is to be used only for the purposes described in the Federal Register.
2. Disclosure. Information about an individual shall not be disclosed to any unauthorized individual. Anyone who makes an unauthorized disclosure on purpose may be fined up to \$5,000 . All DON personnel who maintain records about individuals have an obligation to do their part in protecting personal information from unauthorized disclosure. SECNAVINST 5211.5D describes when disclosures are authorized.
3. Individual Access. Every individual, with certain exceptions, has the right to look at any record which the DON keeps on him/her, to copy it, and to request to have it corrected if he/she considers it wrong. The individual attempting to exercise these rights shall be given courteous and considerate assistance.
4. Ensuring Accuracy. The DON has an obligation to use only accurate, timely, relevant, and complete information when making decisions about individuals. All DON personnel involved in keeping records on individuals shall assist in the discharge of this obligation.



# Privacy Best Practices

**When collecting PII – think about ways to ensure that the personal information you collect and manage is properly protected.**

**REMEMBER --**

- If you collect it – you must protect it!**
- If in doubt – leave it out.**
- Just because “it has always been done this way”  
-- does not mean it is still the best way to do it.**



# Review Business Practices

**ASK – Is the data I handle privacy protected?**

- **At a minimum, privacy data should be marked:**  
***“For Official Use Only – Privacy Sensitive: Any misuse or unauthorized disclosure may result in both civil and criminal penalties.”***
- **Be aware that privacy data may not always be properly marked. If you have questions about whether data is protected under the Privacy Act, ask your supervisor or the NRL Privacy Office.**



# Collecting and Storing PII

- **Don't place PII in public folders in Outlook for others to view.**
- **Don't place PII information on public web sites.**
- **Don't collect duplicate information -- if you have it somewhere else, you don't need to collect it again.**



# Methods for Safeguarding PII

- Follow OMB guidance's security requirements:
  - ❖ Encrypt sensitive information – makes it unreadable for unauthorized people.
  - ❖ Provide controls regarding remote access –present 2 ways to prove that the user has authorized access.
  - ❖ Provide a time-out function for information systems – after a period of no more than 30 minutes of inactivity, the user would be required to log-in again.
- Reduce and eliminate the unnecessary collection of Social Security Numbers (SSN). Federal agency organizations must participate in government-wide efforts to explore other options to agency use of Social Security numbers as personal identifiers for both Federal employees and in Federal programs.
- Ensure all authorized individuals sign a document that they have reviewed their responsibilities to safeguard PII.



# Best Practices for Safeguarding Sensitive PII

## Email

- All email containing sensitive PII must be digitally signed and encrypted using DoD-approved certificates.
- Send the password separately via email, or telephone the recipient with the password.
- Ensure the email subject line contains "FOUO – Privacy Sensitive," and the body of the email contains the following language:

**FOUO – Privacy Sensitive Information. Any misuse or unauthorized disclosure may result in both civil and criminal penalties.**



# Best Practices for Safeguarding Sensitive PII

## Intra-Lab Printed Materials

- Double wrap documents containing sensitive PII.
- Never simply use “holey joes,” and do not indicate on the envelope that it contains PII.
- Instead, mark the envelope “Eyes Only” and to the attention of the authorized recipient.
- As a best practice, use DD Form 2923 “Privacy Act Data Cover Sheet” as a cover sheet to the printed material.
- Mark documents that contain sensitive PII: FOUO –Privacy Sensitive Information. Any misuse or unauthorized disclosure may result in both civil and criminal penalties.



# Best Practices for Safeguarding Sensitive PII

- **FAX.** Double check fax numbers before sending and call ahead and ensure that someone is standing by to receive the fax. Properly mark your documents: FOUO – Privacy Sensitive. Any misuse or unauthorized disclosure may result in both civil and criminal penalties.
- **Printing/Copying.** When making copies of documents containing sensitive information, remember to retrieve the originals and all copies from the copier. Retrieve documents containing sensitive information from shared printers as soon as they are printed. When available, print to printers located in secured rooms.
- **Shared Drives.** Store, save, and use sensitive PII on “shared drives” only if access is restricted to those with a “need to know” by permission settings or passwords



# Best Practices for Safeguarding Sensitive PII

## IT Equipment

- Never leave your laptop unattended.
- Encrypt the entire laptop so that sensitive PII will not be compromised if the laptop is lost or stolen.
- Mobile electronic equipment – such as flash drives, CDs, or other storage media – must be encrypted.
- Never store PII on personal devices; use only Government furnished equipment (GFE), including while teleworking.
- Do not maintain PII on a public Web site or electronic bulletin board.
- Mark all external drives or mobile media with FOUO – Privacy Sensitive. Any misuse or unauthorized disclosure may result in both civil and criminal penalties



# Best Practices for Safeguarding Sensitive PII

## In the Mail

- For mailings containing a small amount of sensitive PII (such as for an individual employee action): seal sensitive PII materials in an opaque envelope or container and mail using the U.S. Postal Service's First Class Mail, Priority Mail, or an accountable commercial delivery service.
- For large data extracts, database transfers, backup tape transfers, or similar collections of sensitive PII: encrypt and use a receipted delivery service (e.g., Return Receipt, Certified or Registered mail) or a tracking service to ensure secure delivery is made to the appropriate recipient.



# Best Practices for Safeguarding Sensitive PII

## Physically secure sensitive PII

- When not in use or otherwise under the control of a person with a need to know, properly secure in a *locked* drawer, cabinet, or desk.
- When in transit. Do not mail or courier Sensitive PII on CDs, DVDs, hard drives, flash drives, USB drives, floppy disks, or other removable media unless the data is encrypted.

And, finally –

**If someone sends you sensitive PII in an unprotected manner, you still must secure it once you receive it.**



# Soliciting PII

## When soliciting PII from an individual . . .

- Agencies are required to provide a Privacy Act Statement to all persons asked to provide personal information about themselves that will go into a system of records (i.e., the information will be stored and retrieved using the individual's name or other personal identifier such as SSN). This is true no matter the method used to collect the information: forms, in person, telephone interview, etc.
- In such a case, a Privacy Act Statement that addresses the authority for the collection, purpose for the collection, routine uses that will be made of the information, and whether the collection is voluntary or mandatory must be provided.
- If you have any questions about this, please contact the NRL Privacy Act Coordinator.



# Example of a Privacy Act Statement

## **PRIVACY ACT STATEMENT [Request for Variable or First-40-Hour Work Schedule Instructions]**

**AUTHORITY:** Section 6311 of Title 5, United States Code, authorizes collection of this information.

**PRINCIPLE PURPOSE:** The primary use of this information is by management and your payroll office to approve and record your work schedule.

**ROUTINE USES AND DISCLOSURE:** Additional disclosures of this information may be to: the Department of Labor when processing a claim for compensation regarding a job connected injury or illness; to a State unemployment compensation office regarding a claim; to Federal Life Insurance or Health Benefits carriers regarding a claim; to a Federal, State or local law enforcement agency when your agency becomes aware of a violation or possible violation of civil or criminal law; to a Federal agency when conducting an investigation for employment or security reasons; to the Office of Personnel Management or the General Accounting Office when the information is required for evaluation of leave administration; or the General Services Administration in connection with its responsibilities for records management.

Furnishing this information is voluntary, but failure to do so may delay or prevent action on this application.



# Distributing Information

- Under the Privacy Act, only individuals with an official need to know may have access to the portion of a record required for that use.
- If a “routine use” disclosure is made outside the DOD, the recipient and purpose must be identified in the SORN. For example, “To the Department of Veteran’s Affairs for the purpose of providing medical care.”
- All disclosures outside the DOD require a disclosure accounting. For example: I gave it to [agency/activity] for [the purpose of ] on [date]. Disclosures should be maintained in the file using a Disclosure Accounting Form or other auditable record.
- Consult your System Manager (in most cases, your AO) if you do not know the system rules for information you manage.



# Destroying Sensitive PII Materials

When should I destroy sensitive PII materials?

- **Sensitive PII, including archived emails that contain sensitive PII, shall be destroyed when retention of the data is no longer required consistent with applicable record retention schedules, or as identified in the applicable system of records notice (SORN) published in the *Federal Register*.**
- **Please see NRLINST 5212.3C, RECORDS RETENTION AND DISPOSAL PROGRAM**



# Destroying Sensitive PII Materials

## How should I dispose of sensitive PII?

- Printed material can be destroyed using a cross-cut shredder, put in “burn bags,” or equivalent destruction means. A disposal method is considered adequate if it renders the material unrecognizable or beyond reconstruction.
- Do not use recycle bins for this purpose.
- Remember to secure sensitive PII that has been discarded in burn bags that are awaiting removal, shredding, or destruction.
- All media that contain or may contain PII must be destroyed rather than discarded in the trash



# Reporting Incidents

**If you suspect or have an actual loss or compromise of PII ...**

- Contact your Privacy Act Coordinator and/or supervisor as soon as you suspect or have an actual loss or compromise of PII.
- Within one hour of discovery, breaches must be reported to US-CERT and your chain of command in accordance with DON CIO guidance.
- The DON CIO will provide the reporting command with a written notification determination.
- If your PII is compromised, monitor financial accounts for suspicious activity.
- If your identity is stolen, immediately contact the Federal Trade Commission (FTC) for more information: [www.ftc.gov](http://www.ftc.gov) or 1-877-IDTHEFT.



# PENALTIES

- **There are criminal penalties addressed under the Privacy Act. They are based on knowingly and willfully:**
  - **Obtaining records under false pretenses.**
  - **Disclosing privacy data to any person not entitled to access.**
  - **Maintaining a system of records without meeting public notice requirements.**
- **Result: Misdemeanor criminal charge and a fine of up to \$5000.**



# PENALTIES

- **Courts may also award civil penalties for:**
  - Unlawfully refusing to amend a record.
  - Unlawfully refusing to grant access to a record.
  - Failure to maintain accurate, relevant, timely, and complete information.
  - Failure to comply with any PA provision or agency rule that results in an adverse effect on the subject of the record.
- **Penalties for these violations include:**
  - Actual damages
  - Payment of reasonable attorney's fees
  - Removal from employment



# Preventative Measures

- Training. All DON personnel who handle PII must complete annual PII training, and the command must maintain auditable certificates of completion.
- Spot Checks. All offices that handle PII must complete a Compliance Spot Check twice yearly, and the command must maintain auditable records.



# Information for Teleworkers

## Teleworkers ...

- Any teleworker who will be working on sensitive PII data must receive appropriate Privacy Act training before teleworking.
- Teleworkers are responsible for the security of all sensitive PII data taken out of the traditional work site; sensitive PII data may not be disclosed to anyone except those authorized access as a requirement of their official responsibilities.
- Only copies, not originals, of sensitive PII documents may be taken out of the traditional work site, and may be taken only on temporary basis and not permanently stored out of the traditional work site.
- Government-furnished computer equipment, software, and communications, with appropriate security measures, are required for any telework arrangement that involves sensitive PII.



# Summary of PA Responsibilities

- **Maintain only accurate, timely, relevant and complete information on individuals.**
- **A Privacy Act Statement must be provided when directly soliciting personal information, stating the authority for the collection, purpose for the collection, routine uses for the information, and whether the collection is voluntary or mandatory.**
- **Follow the guidance set forth in the Systems of Record Notice (SORN) regarding release/withholding of information.**
- **Other than exceptions provided for in the PA (e.g., law enforcement) no disclosure of information should be made without the subject's written consent.**



# PRIVACY TOOLBOX

- <http://hroffice.nrl.navy.mil/privacy.htm>. This is an NRL Privacy Office website that includes information and links on applicable guidance and training. It also links to the DON Privacy Office website, <http://privacy.navy.mil>, which serves as a one stop shop on privacy issuances, policies, guidance, systems of records notices, etc.
- SECNAVINST 5211.5E, DON Privacy Program.
- NRLINST 5211.2F, NRL Privacy Program. All NRL policies and procedures should integrate NRL and DON guidance on privacy act protections.
- Ask your supervisor or Privacy Officer if you have any questions or need more information on how personal information is maintained and used. You may also email the NRL Privacy Office at [PRIVACY@nrl.navy.mil](mailto:PRIVACY@nrl.navy.mil).



# Further Information

NRL Privacy Act Program Manager:

**Kim Thomas, 202-767-2957, [kim.thomas@nrl.navy.mil](mailto:kim.thomas@nrl.navy.mil)**

NRL Privacy Act Coordinator:

**Linda Owens, 202-767-8218, [linda.owens@nrl.navy.mil](mailto:linda.owens@nrl.navy.mil)**

For further information:

**Please review NRL Instruction 5211.2F, Privacy Act Policy and Responsibilities; or email the Privacy Desk at [privacy@hro1.nrl.navy.mil](mailto:privacy@hro1.nrl.navy.mil)**

References:

- DON Users' Guide to PII v2.0 October 2009
- DON breach reporting: DON CIO 291652Z Feb 08
- Privacy Act of 1974, as amended (5 U.S.C. 552a)
- DoD Directive 5400.11, "DoD Privacy Program," May 8, 2007
- DoD Regulation 5400.11-R, "DoD Privacy Program," May 14, 2007



# Thank you for your cooperation.

- You have completed your required annual refresher training under the Privacy Act.
- On the next slide, you will be asked to certify your receipt of this training and your understanding of your Privacy Act responsibilities.
- If you are not currently logged in using your Common Access Card (CAC), you will need to submit a printed and signed copy of your course completion certificate to your Administrative Officer.
- If you are currently logged in using your Common Access Card (CAC), your CAC card is your electronic signature of completion and you do not need to submit a completion certificate to your Administrative Officer.



# CERTIFICATION OF ANNUAL REFRESHER TRAINING 2015

***This is to certify that I have received annual training on my privacy responsibilities. I understand I am responsible for safeguarding personally identifiable information (PII) while performing official duties. I also understand that I may be subject to disciplinary action for failure to properly safeguard PII, improperly using or disclosing PII, and for failure to report a known or suspected loss of PII.***

☐ By checking this box you are certifying the completion of this Privacy Act training and acknowledging your responsibility to comply with any regulations, policies and procedures prescribed within.

~~~

**If you are not currently logged in using your Common Access Card (CAC), you will need to submit a printed and signed copy of your course completion certificate to your Administrative Officer. Otherwise, your CAC card is your electronic signature of completion.**

**Sign:** \_\_\_\_\_

**DATE:** \_\_\_\_\_